日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　９月２７日

出願番号
Application Number:　特願２００２－２８２８４２

[ST.10/C]:　[ＪＰ２００２－２８２８４２]

出願人
Applicant(s):　新潟大学長

２００３年　１月２８日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３００２０８６

【書類名】　特許願
【整理番号】　U2002P088
【提出日】　平成14年 9月27日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F　7/56
【発明の名称】　乱数発生方法及び乱数発生装置
【請求項の数】　9
【発明者】
　【住所又は居所】　新潟県新潟市五十嵐一の町７７９４番地２０
　【氏名】　斉藤　義明
【特許出願人】
　【識別番号】　596133441
　【氏名又は名称】　新潟大学長　長谷川　　彰
【代理人】
　【識別番号】　100072051
　【弁理士】
　【氏名又は名称】　杉村　興作
【選任した代理人】
　【識別番号】　100059258
　【弁理士】
　【氏名又は名称】　杉村　暁秀
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9812710
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　乱数発生方法及び乱数発生装置

【特許請求の範囲】

【請求項１】　第１のトランジスタと第２のトランジスタとを具える双安定性マルチバイブレータ回路に対して駆動電圧を印加することにより、前記第１のトランジスタ又は前記第２のトランジスタをランダムにオンオフさせ、前記第１のトランジスタ又は前記第２のトランジスタのオンオフ状態に対応させて０又は１の数字を割り当て、２進数的な乱数を発生させるようにしたことを特徴とする、乱数発生方法。

【請求項２】　前記第１のトランジスタ又は前記第２のトランジスタの前記オンオフ状態は、前記第１のトランジスタ又は前記第２のトランジスタのコレクタ電圧を計測することによって検出することを特徴とする、請求項１に記載の乱数発生方法。

【請求項３】　前記双安定性マルチバイブレータ回路の回路部品の特性値を調節することにより、０及び１の生起確率を制御するようにしたことを特徴とする、請求項１又は２に記載の乱数発生方法。

【請求項４】　０及び１の生起確率を０．５にすることを特徴とする、請求項３に記載の乱数発生方法。

【請求項５】　前記回路部品はバイアス可変抵抗であり、この抵抗の抵抗値を調節することを特徴とする、請求項３又は４に記載の乱数発生方法。

【請求項６】　双安定性マルチバイブレータ回路を具えることを特徴とする、乱数発生装置。

【請求項７】　前記双安定性マルチバイブレータ回路は、バイアス可変抵抗を含むことを特徴とする、請求項６に記載の乱数発生装置。

【請求項８】　前記双安定性マルチバイブレータ回路に接続され、前記双安定性マルチバイブレータ回路に対する駆動電圧を生成するための電源制御回路を具えることを特徴とする、請求項６又は７に記載の乱数発生装置。

【請求項９】　前記双安定性マルチバイブレータ回路の前記第１のトランジスタ又は前記第２のトランジスタのコレクタ側に接続され、前記第１のトランジスタ

又は前記第２のトランジスタのコレクタ電圧を取り出すためのバッファ回路を具えることを特徴とする、請求項６～８のいずれか一に記載の乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号作製技術などの情報産業分野、特に将来の量子コンピュータなどの分野において好適に用いることのできる乱数発生方法及び乱数発生装置に関する。

【０００２】

【従来の技術】

完全に無秩序であり、かつ全体としては出現頻度が等しくなる乱数は、社会現象や物理現象の数値シュミレーションなどに広く利用されている。また、乱数は暗号技術としても重要な役割を果たしており、情報の保護の分野でもその需要が高い。現在、乱数の発生方法として種々の方法が開発されているが、そのほとんどはアルゴリズムによるソフト的な疑似乱数の生成である。

【０００３】

アルゴリズムによる乱数生成は、ある程度の信頼性を有し、高速に乱数生成を行なうことができるという点から広く利用されている。しかしながら、コンピュータは有限の情報しかとらないために、生成された乱数は周期性を持つことが確認されている。そのため、正確な解や十分なセキュリティが得られない場合があり、より無秩序な乱数発生方法の確立が望まれている。

【０００４】

近年、ハードウエアの発展に伴う処理速度の向上と信頼性の向上から、物理的な乱数の生成方法が開発されてきた。例えば、熱電子雑音や放射性物質の崩壊などの物理現象に基づいて生成された乱数は、予測不可能性の高い、理想的な乱数列であることが知られている。しかしながら、これらの方法では高価で大掛かりな装置を必要とすることが多い。

【０００５】

【発明が解決しようとする課題】

本発明は、廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上記目的を達成すべく、本発明は、第１のトランジスタと第２のトランジスタとを具える双安定性マルチバイブレータ回路に対して駆動電圧を印加することにより、前記第１のトランジスタ又は前記第２のトランジスタをランダムにオンオフさせ、前記第１のトランジスタ又は前記第２のトランジスタのオンオフ状態に対応させて０又は１の数字を割り当て、２進数的な乱数を発生させるようにしたことを特徴とする、乱数発生方法に関する。

【０００７】

また、本発明は、双安定性マルチバイブレータ回路を具えることを特徴とする、乱数発生装置に関する。

【０００８】

双安定性マルチバイブレータ回路は、一般に個別部品回路の状態であっても集積回路の状態であっても、前記回路を構成する２個のトランジスタの正帰還結合によって構成されている。前記双安定性マルチバイブレータにおいては、駆動電圧を印加した瞬間に、前記２個のトランジスタの一方が導通し、他方は遮断状態となる。したがって、前記２個のトランジスタの特性及び回路部品の特性が完全に一致して、理想的な双安定性マルチバイブレータ回路を構成している場合は、前記２個のトランジスタのどちらが導通するかを予測することは不可能になり、前記双安定性マルチバイブレータ回路内に存在する雑音に依存して決定される。

【０００９】

したがって、前記２個のトランジスタの一方の導通状態を検出し、例えば導通状態の場合に数字の“０”を対応させ、遮断状態の場合に数字の“１”を対応させるようにすれば、前記トランジスタのオンオフは前記双安定性マルチバイブレータ回路内に存在する雑音によりランダムとなるから、２進数的な乱数を発生させることができるようになる。

【００１０】

なお、前記トランジスタのオンオフ状態は、そのコレクタ電圧を計測することによって簡易に検出することができる。

【００１１】

また、上述したような理想的な双安定性マルチバイブレータ回路を構成することができない場合においては、前記トランジスタのオンオフを完全にランダム化することは困難になり、一般には導通状態又は遮断状態のどちらかの状態に偏ることになる。したがって、このような場合においては、上述したような２進数的な乱数を発生させることが困難になる。

【００１２】

このような場合においては、前記双安定性マルチバイブレータ回路内の回路部品の特性値を調節し、前記トランジスタのオンオフ状態が前記回路内の雑音に依存してランダムとなるように制御することが好ましい。特には、ある一定期間内でのオンオフ状態が同じ確率でランダムに生じるようにすることが好ましい。これによって、前記期間内での“０”及び“１”の生起確率が０．５となり、２進数的な乱数を発生させることができるようになる。

【００１３】

【発明の実施の形態】

以下、本発明を発明の実施の形態に基づいて詳細に説明する。

図１は、本発明の乱数発生装置に含まれる双安定性マルチバイブレータ回路の一例を示す回路図である。図１に示す回路においては、トランジスタＴ１及びＴ２、コレクタ抵抗Ｒ１及びＲ２、帰還抵抗Ｒ３及びＲ４、並びにバイアス抵抗Ｒ７、Ｒ８、Ｒ９及びＲ１１が基本的な回路部品であり、コンデンサＣ１及びＣ２、抵抗Ｒ５及びＲ６、並びにダイオードＤ１～Ｄ４は波形成形の目的で付加されているものであり、付属的な回路部品である。

【００１４】

双安定性マルチバイブレータ回路として機能させるべく、トランジスタＴ１及びＴ２は、同一の特性を有するトランジスタから構成する。また、コレクタ抵抗Ｒ１及びＲ２の抵抗値、帰還抵抗Ｒ３及びＲ４の抵抗値、並びにコンデンサＣ１及びＣ２のキャパシタは、それぞれ同一となるように設定する。なお、抵抗値Ｒ

５及びＲ６、並びにダイオードＤ１～Ｄ４の特性は必ずしも同一とすることは要求されない。但し、一般的にはこれらの回路部品の特性についても同一に設定する。

【００１５】

図１に示す双安定性マルチバイブレータ回路に対して所定の駆動電圧を“入力”側から印加すると、トランジスタＴ１又はＴ２のどちらか一方が導通状態となり、他方が遮断状態となる。このとき、トランジスタＴ１及びＴ２の特性、コレクタ抵抗Ｒ１及びＲ２の抵抗値、帰還抵抗Ｒ３及びＲ４の抵抗値、コンデンサＣ１及びＣ２のキャパシタ、並びにバイアス抵抗Ｒ８及びＲ９＋Ｒ１１の抵抗値が完全に一致していれば、トランジスタＴ１及びＴ２のオンオフ状態は予測することができず、これらトランジスタのオンオフ状態は双安定性マルチバイブレータ回路内に存在する雑音に依存して決定される。

【００１６】

したがって、トランジスタＴ１がオンとなって導通状態の時に数字の“０”を対応させ、トランジスタＴ１がオフとなって遮断状態の時に数字の“１”を対応させるようにする。前述したように、トランジスタＴ１のオンオフ状態は前記双安定性マルチバイブレータ回路内に存在する雑音に依存するので、“０”及び“１”の数字がランダムに生成され、２進数的な乱数を発生させることができるようになる。

【００１７】

トランジスタＴ１のオンオフ状態は、例えばトランジスタＴ１のコレクタ電圧を“出力”側を通じて計測するようにすれば簡易に検出することができる。

【００１８】

しかしながら、上述したような理想的な双安定性マルチバイブレータ回路は、トランジスタＴ１及びＴ２などの特性を一致するようにした場合においても実現することが困難であり、一般的にはトランジスタＴ１及びＴ２はオン状態又はオフ状態に傾動する傾向がある。したがって、乱数発生のためのコレクタ電圧を検出すべきトランジスタＴ１は、導通状態又は遮断状態である場合が遮断状態又は導通状態にある場合よりも多くなり、“０”又は“１”の数字が生起される確率

が“１”又は“０”の数字が生起される確率よりも多くなる。その結果、２進数的な乱数を発生させることができなくなる。

【００１９】

このような場合において、双安定性マルチバイブレータ回路内の回路部品の特性を調節することにより、ある一定の期間内において、トランジスタＴ１及びＴ２のオンオフ状態が等確率（０．５）で出現するようにする。この場合においては、上述したように、双安定性マルチバイブレータ回路の雑音に依存して、トランジスタＴ１は、導通状態及び遮断状態をランダムに採るようになるので、これらの状態に“０”及び“１”の数字を割り当てることにより、“０”及び“１”の生起確率は０．５となり、２進数的な乱数を発生できるようになる。

【００２０】

図１においては、例えば可変抵抗であるバイアス抵抗Ｒ１１の抵抗値を制御することによって、トランジスタＴ１及びＴ２のオンオフ状態を等確率で出現させることができる。

【００２１】

図２は、図１に示す双安定性マルチバイブレータ回路に印加すべき駆動電圧を発生させるための、電源制御回路の一例を示す回路図である。図２に示す電源制御回路は、その出力側を図１に示す双安定性マルチバイブレータ回路の入力側に直列に接続する。

【００２２】

図２に示す電源制御回路は、電源より所定のバイアス電流が導入されるとともに、所定の矩形波がコンデンサＣ３及びＣ４を介して導入され、トランジスタＴ３をスイッチング動作させることによって、トランジスタＴ３のコレクタ側に双安定性マルチバイブレータ回路に対する駆動電圧を発生させ、出力する。なお、コンデンサＣ３及びＣ４の代わりに単一の無極性コンデンサを用いることもできる。

【００２３】

図３は、図１に示す双安定性マルチバイブレータ回路のトランジスタＴ１のコレクタ電圧を出力し、計測するために用いるバッファ回路の一例を示す回路図で

ある。図３に示すバッファ回路は、その入力を図１に示す双安定性マルチバイブレータ回路におけるトランジスタＴ１のコレクタ側に設けられた出力と接続する。そして、バッファ回路の出力側から計測したコレクタ電圧値を外部に取り出し、所定の演算処理などに供する。

【００２４】

このようなバッファ回路を設けることにより、双安定性マルチバイブレータ回路に影響を与えることなく、トランジスタＴ１のコレクタ電圧値を計測することができるようになる。したがって、２進数的な乱数を安定的に発生させることができるようになる。

【００２５】

図４及び図５は、図１～図３から構成される乱数発生装置を用いて乱数発生の実験を行なった際の実験結果を２次元的に表示したものである。図４は５０００個の乱数を表し、図５は１００００個の乱数を表している。図４及び図５には格子縞などが発生することなく、点状の分布が見られるのみで、２進数的な乱数が生起されていることが分かる。

【００２６】

以上、具体例を挙げながら発明の実施の形態に基づいて本発明を詳細に説明してきたが、本発明は上記内容に限定されるものではなく、本発明の範疇を逸脱しない限りにおいて、あらゆる変形や変更が可能である。

【００２７】

例えば、図１に示す回路図において、入力端子及びアース間に適当なキャパシタを適当な値に設定したコンデンサＣ１１（０．００１μＦ）、Ｃ１２（０．１μＦ）及びＣ１３（１μＦ）を並列に接続することにより、動作の安定性を向上させることができる。また、上記においてはトランジスタＴ１のオンオフ状態に対応させて２進数的な乱数を発生させたが、トランジスタＴ１に代えてトランジスタＴ２を用いることもできる。

【００２８】

さらに、トランジスタＴ１及びＴ２のバランスを取る可変抵抗器Ｒ１１は、抵抗Ｒ９に対して直列に接続するのみならず、並列に接続することもできる。また

、Ｒ１１に代えて他の可変抵抗を用い、これを図１に示す双安定性マルチバイブレータ回路の任意の抵抗に対して直列又は並列となるように接続するような構成を採ることもできる。

【００２９】

【発明の効果】

以上説明したように、本発明によれば、廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供することができる。

【図面の簡単な説明】

【図１】　本発明の乱数発生装置に含まれる双安定性マルチバイブレータ回路の一例を示す回路図である。

【図２】　双安定性マルチバイブレータ回路に印加すべき駆動電圧を発生させるための、電源制御回路の一例を示す回路図である。

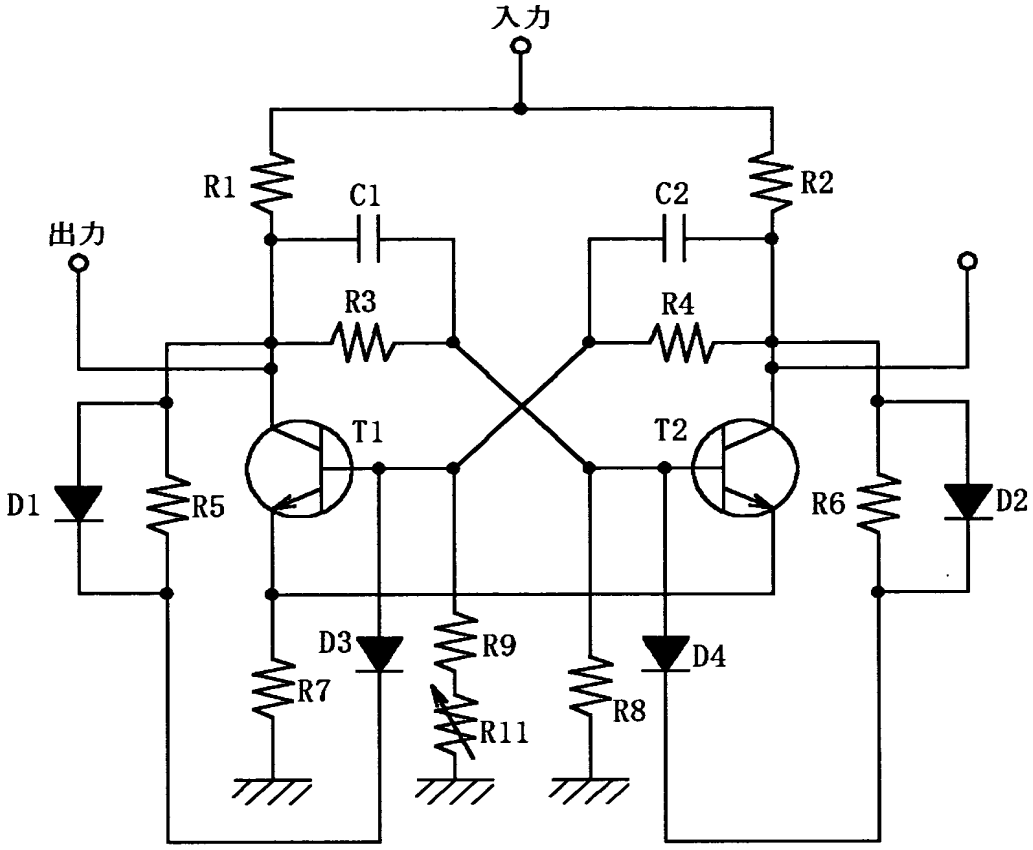
【図３】　双安定性マルチバイブレータ回路のトランジスタのコレクタ電圧を出力し、計測するために用いるバッファ回路の一例を示す回路図である。

【図４】　本発明の方法及び装置を用いて生起した乱数の２次元度数分布図である。

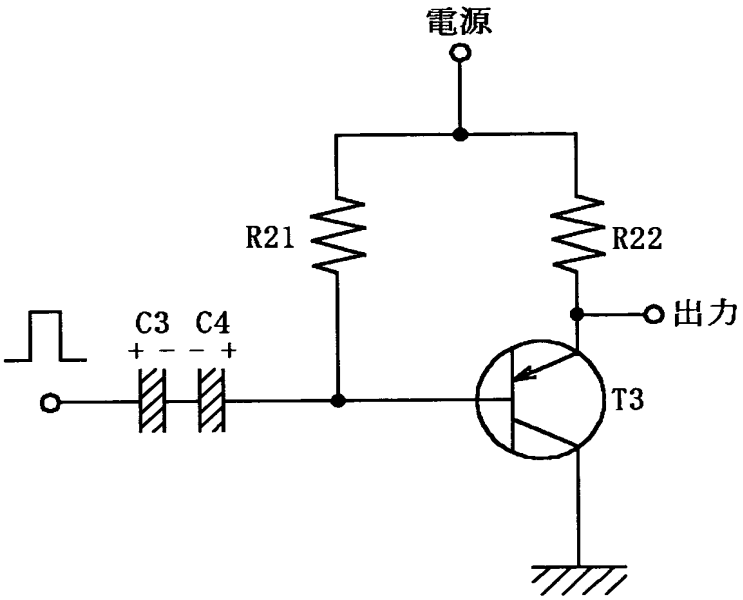
【図５】　本発明の方法及び装置を用いて生起した乱数の２次元度数分布図である。

【書類名】　　図面

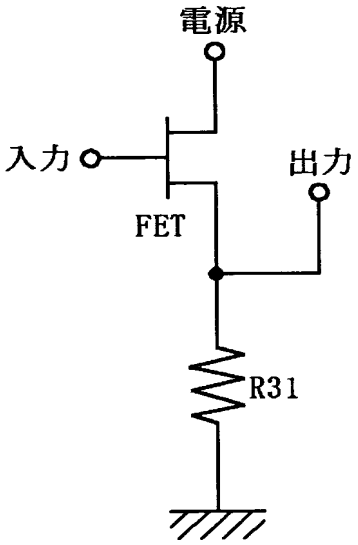
【図１】



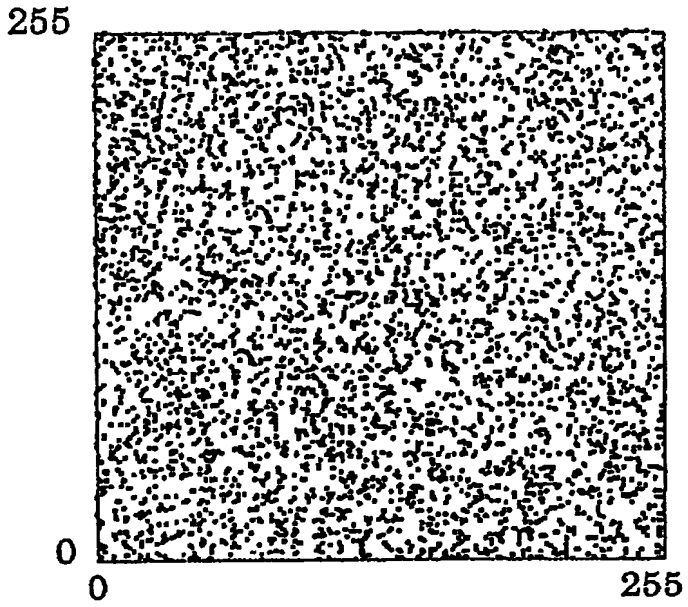
【図２】



【図３】

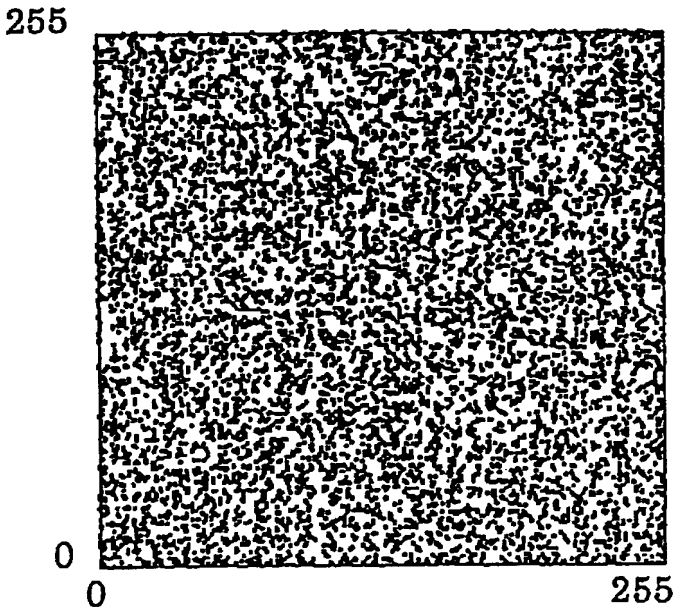


【図４】



(n=5,000)

【図５】



(n=10,000)

【書類名】　　要約書

【要約】

【課題】　廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供する。

【解決手段】　双安定性マルチバイブレータ回路に対して所定の駆動電圧を“入力”側から印加して駆動させる。このとき、トランジスタのオンオフ状態は、前記双安定性マルチバイブレータ回路内の雑音に依存してランダムに発生するようになるので、前記トランジスタの導通状態（オン状態）及び遮断状態（オフ状態）に対応させて、数字の“０”及び“１”をそれぞれ対応させることにより、２進数的な乱数を発生させる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００２－２８２８４２
受付番号	５０２０１４５２３９９
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年　９月３０日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	596133441
【住所又は居所】	新潟県新潟市五十嵐２の町８０５０番地
【氏名又は名称】	新潟大学長

【代理人】　申請人

【識別番号】	100072051
【住所又は居所】	東京都千代田区霞が関３－２－４　霞山ビル７階
【氏名又は名称】	杉村　興作

【選任した代理人】

【識別番号】	100059258
【住所又は居所】	東京都千代田区霞が関３－２－４　霞山ビル７階
【氏名又は名称】	杉村　暁秀

次頁無

出証特２００３－３００２０８６

出　願　人　履　歴　情　報

識別番号　　〔５９６１３３４４１〕

１．変更年月日　　１９９６年　９月１１日
［変更理由］　新規登録
住　所　　新潟県新潟市五十嵐２の町８０５０番地
氏　名　　新潟大学長